



Commentary

Control Over Personal Information in the Database Era

Mark Andrejevic

Department of Communication Studies, University of Iowa, USA, <mailto:mark-andrejevic@uiowa.edu>

In February 2009 the House of Lords Constitutional Committee in the United Kingdom published the report *Surveillance: Citizens and the State*. Some have hailed this as a landmark document. The following is one of four commentaries that the editors of *Surveillance & Society* solicited in response to the report.

If it is the thought that counts – and it should count for something – the attempt by the House of Lords and other elements of the British Government to focus attention on surveillance issues is a welcome one. There is little doubt that surveillance in its various forms is destined to become a central policy issue in the digital era, and it is equally clear that some of the ready-to-hand ways of thinking about issues of state monitoring, market research, and personal privacy are hopelessly outdated. The recommendation in the House of Lords report to, “involve schools, learned and other societies, and voluntary organisations in public discussion of the risks and benefits of surveillance and data processing,” should be taken as a challenge to rethink surveillance issues in ways that are as broad-ranging and comprehensive as the dramatic transformations in surveillance practices we are currently facing. This response to the report highlights in particular the importance of rethinking the relationship between private and public sector surveillance, of confronting the permeation of social space by market-driven forms of monitoring, and of interrogating the simple opposition between freedom and surveillance that characterizes some of the report’s formulations.

To its credit, the report repeatedly expresses concern over the failure to grant the Privacy Commissioner’s Office the power to monitor private sector compliance with regulations governing the handling of personal information. It also acknowledges, in passing, the “growing exchange of personal data between the public and private sectors” (58). What bears further exploration, however, is the eroding boundary between *modes* of surveillance – the adoption by both private and public sectors of actuarial models for managing risk and data-driven customization systems for providing services. In both cases, surveillance takes on a particular meaning: the creation of a comprehensive data portrait of an entire population. No longer is there a distinction between surveillance targets and non-targets: the population itself is the target, and each member of the population an integral part of the overall picture.

As Professor Clive Norris put it in his comments to the report committee, the switch from targeting individuals to monitoring populations, “becomes in a sense expansionary to a huge degree. If you see that information is what you need to solve a problem, but you do not quite know what that problem is and you do not know what future events you are going to be responding to, the temptation is to collect all information about all people” (28). In the petabyte era, this observation can be put even more forcefully: collecting information about everyone becomes not just a technological temptation, but an operational necessity – a different way of doing surveillance.

Andrejevic, Mark. 2009. Control Over Personal Information in the Database Era. *Surveillance & Society*, 6(3): 322-326. <http://www.surveillance-and-society.org> | ISSN: 1477-7487

© The author(s), 2009 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Invoking the term popularized by Ian Ayres (2007), database forms of monitoring, whether for law enforcement, marketing, or providing services, rely on the process of “super-crunching” as much information as possible in order to generate robust predictive patterns. In such a context it becomes as important to collect information about non-targets as potential targets (of suspicion or services) in order to set norms and to unearth new correlations. What is at stake here – in both marketing and law enforcement — is a shift to a model in which conventional standards for evaluating targeted surveillance are, in a sense, sidelined. As the report puts it, in the era of data-mining and profiling, “the use of personal data in data matching and profiling presents challenges to the necessity and proportionality aspects of data protection and human rights legislation” (14). For example, the report describes the use of covert surveillance, hidden cameras or recording devices to catch litterbugs as a representative case of non-proportional surveillance. But, when the model shifts from one based on targeted surveillance to data-mining, the structure of accountability standards changes. No longer is it a question of whether or not to subject a particular individual to a specific monitoring regime. In a database model individual targets emerge *after the fact* as outputs of the surveillance process. Thus, the pertinent decision becomes whether or not to use a population-driven database model – and in many cases that choice has already been made.

The standards for regulating surveillance in the database era shift accordingly: we need to consider how monitoring systems can be designed in ways that enhance citizen control and facilitate accountability. Similarly, the notion of individual or personal autonomy needs to be supplemented by a conception of “collective autonomy.” As a society, what level of customization and targeting are we comfortable with? What types of data queries do we want to rule out of bounds? How do we want data sharing processes to be structured? How do we avoid the pathologies of discrimination and disempowerment associated with the sorting process? To date, the default assumption in both the public and private sectors has been that if some customization is good, more is better. This assumption needs to be revisited at the level of public policy and public deliberation. If personal autonomy can be understood as, among other things, entailing control over the disclosure of personal information, the process of building regulatory structures that secure this autonomy must take place at the collective level. In this regard, the report provides welcome recognition that freedom, in a meaningful sense, cannot be secured by aggregating individual “free” choices in the marketplace, but must be addressed at the level where market relations are themselves structured – that is, at the regulatory level.

In practice, however, the rampant privatization of interactive spaces pushes in the opposite direction. The failure to directly address this process is one of the report’s blind spots. What we are facing, in the realms of content provision and interpersonal communication, might be described as a virtual version of the privatization of social space. If the second half of the 20th century witnessed the increasing privatization of physical space, from the process of suburbanization to the replacement of downtown shopping areas by shopping malls, the first half of the 21st century continues the trend in virtual space. Applications like Facebook, MySpace, and Gmail facilitate the 21st century’s ongoing privatization of the social space of communication.

Two intertwined processes are at work in this form of privatization, both of which have implications for the critique of a so-called surveillance society. The first is the development of interactive forms of monitoring facilitated by networked digitization. To take one example, as e-mail comes to replace the Royal Mail for a variety of uses (though certainly not all uses), written correspondence is subjected to more comprehensive and exhaustive forms of monitoring, data collection, and storage. Unlike the Royal Mail, Gmail can keep copies of the contents of every message sent using its service, and keep detailed records of when and where the e-mail service is used, when messages are read, responded to, and discarded. In the case of Gmail, the contents of all messages can be mechanically scanned for keywords. The move from “snail mail” to email thus represents a quantum leap in the ability to monitor consumer behaviour. Since users may be more likely to correspond more frequently and rapidly over email, they generate more grist for the data mill. The ease of email, in other words, helps transform written communication in ways that accelerate interactions even as they generate more data for monitoring systems. The same can be said of other applications that privatize socialization, communication, and

information gathering. As the report suggests, however, increasing privatization goes hand-in-hand with the de-differentiation of private and public sector forms of monitoring. The private sector may be taking the lead in accumulating demographic, psychographic, geographic, and other forms of transactionally generated data, but in so doing it draws the attention of state surveillance systems. As the private sector takes on security duties offloaded onto it by the state, and as the state adopts actuarial models of surveillance for both law enforcement and service provision, the result is, ‘the growing exchange of personal data between the public and private sectors,’ noted in the report (103). The process is exacerbated by the tendency of state agencies, especially in the wake of the September 11 attacks, to view commercial databases as treasure troves of raw data for law enforcement and intelligence agencies.

The privatization of information collection means enhanced surveillance goes hand-in-hand with reduced accountability. Thus, the example of the transition from Royal Mail to email also represents a shift from a public to a private infrastructure, from one with built in mechanisms for public accountability to one that may not even be based in the United Kingdom. At the same time, the example of the shift from Royal Mail to email represents a shift from a public to a private infrastructure, from one with built in mechanisms for public accountability to one that may not even be based in the United Kingdom. This shift is a crucial one the implications of which tend to be both under-reported and under-acknowledged. The emerging online commercial model for communication and social networking relies increasingly on targeted advertising and thus on accumulating as much information as possible about individual users. The shift from a public infrastructure to a private one thus means shifting from a fees- and tax-funded system to a commercial model whose ongoing survival depends on increasingly comprehensive surveillance. Surveillance is not ancillary to the online business model; it lies at its very core.

The burgeoning popularity of social networking sites replicates this logic: it represents the migration of increasingly popular forms of socializing and communication into commercially owned and operated network infrastructures. This is not to diminish the new and clearly popular forms of socializing such networks make possible. Rather, it is to point out that they represent the galloping privatization of realms of social life that were once, for the most part, beyond the monitoring gaze of marketers and the state agencies that seek access to private sector databases. It is also to point out that the new frontiers in socializing pioneered by social networking sites and other networked forms of socialization take place within a commercial model based on the collection of comprehensive data about whom users stay in touch with, whom they contact most frequently and how. Such networks make possible the construction of comprehensive data portraits of our social lives. They also facilitate the commercial saturation of our social interactions. The Royal Mail does not insert targeted advertising appeals in our personal correspondence – and it does not track the details of our prose in order to target those ads more effectively. Google does.

The commercialization of our interactive infrastructure is not inevitable but contingent. It is perfectly possible to imagine publicly subsidized Internet service providers, social networking sites, and e-mail applications; indeed, this was the original model for e-mail communication. Increasingly, however, we are living in a world in which the accepted default model for networked forms of interaction is a privatized one with profound implication for private sector forms of monitoring. Whereas it once might have seemed intrusive or worse to find ourselves turning over the details of our social lives to interested marketers, it is now normal practice online, thanks to the naturalization of a mass-customized commercial model for online social utilities.

Concerns about the proliferation of monitoring tend to reinforce the apparent opposition between freedom on one hand and surveillance on the other – especially when the focus is on the state rather than on the private sector (as in the House of Lords report). However terms like “freedom” and “liberty” can be slippery ones that, if undefined, function to obscure rather than clarify the discussion. It is perhaps not surprising, for example, that the report’s critique of state surveillance (repeatedly described as “scathing” in the media coverage), lends itself to appropriation by populist elements on the right as a means of whipping up animosity toward the state. Thus, the report’s repeated tendency to posit a simple opposition

between liberty and surveillance resonates not only with a patrician distaste for the sordid business of snooping, but also with sentiments like those published in the letters section of the *Times of London* in response to the House of Lords's stated concerns about the coming surveillance society: "We are fortunate that the House of Lords (ironically unelected) has the courage to protect the fundamental freedoms we enjoy – unlike Gordon Brown and the Labour party, who want to turn out country into a totalitarian surveillance state" (*The Times* 2009: 29).

The implied opposition of freedom (with the forms of privacy that underwrite it) and surveillance (alongside the security that serves as its alibi) is a recurring theme in the report and the headlines it spawned, including, for example "Ever Increasing Use of Surveillance and Data Collection Risks Undermining Fundamental Freedoms," (*States News Service* 2009) "Surveillance Undermines Freedoms," (*Secure Computing* 2009), and, "Lords: Rise of CCTV is Threat to Freedom" (Travis 2009).

The opposition is not only misleading, but paradoxically runs the danger of undermining protective controls on rapidly expanding forms of surveillance. Controlling surveillance, perhaps not surprisingly, itself relies on forms of monitoring. As David Lyon, among others, has compellingly argued (see, for example, Lyon 2007), surveillance has multiple valences in a democratic society – it can surely be used in ways that reinforce power imbalances, threaten democratic self-governance and individual autonomy, but, as the report notes, it also has an important role to play in allocating resources, protecting citizens, and the process of collective self-governance. Securing individual liberty and personal freedom relies, at least in part, on strategies for monitoring threats to their exercise. Thus it is perhaps not surprising that one of the report's recommendations for limiting state and commercial forms of surveillance is increased monitoring – not least of private corporations that collect, sort, and analyse personal information collected from consumers.

The simplified neo-libertarian equation of state monitoring with authoritarianism plays into the hands of those in the privacy sector who would seek to avoid public scrutiny of their information gathering practices. The unexamined assertion of privacy rights can have the perhaps unanticipated effect of protecting the commercial sector's privatization of personal information. Furthermore, the opposition between surveillance and freedom licenses the post-9/11 assertion that there is a necessary trade-off between the two: that if the public demands more security, it must simultaneously be conceding its willingness to give up some of its freedoms. This makes it all too easy for political leaders to justify unaccountable surveillance schemes rather than imagining how freedom and security might work hand-in-hand. Instead of reproducing an outmoded opposition and its attendant pathologies, we would do better to ask two questions: what forms of surveillance might help to secure and protect the forms of liberty we associate with democratic self-governance, and how might surveillance schemes be implemented in ways that accord with democratic values rather than undermining them? The simple equation of surveillance with authoritarianism is a way to dodge the challenges posed by these questions and, perhaps more disturbingly, conceding that freedom is necessarily in decline as long as risk is on the rise.

The discussion that needs to take place is necessarily a complex and fast-moving one, but a few principles seem clear, including the importance of opposing forms of state surveillance that do not have a built-in record keeping and disclosure provision (even if disclosure need be delayed for security or other purposes). Thus, for example, measures like the infamous USA Patriot act which enhanced state monitoring capacities while exempting them from sunshine laws (that allow citizens and the press access to government records), centralize power and subvert democratic forms of accountability. When it comes to both state and private sector surveillance the principles of transparency, accountability (even if it is to other government agencies), notification when monitoring is taking place, and correction (the ability of citizens to see and correct data about themselves), are basic. However, they do not in themselves regulate the level of customization and anonymity available to citizens. The emerging private sector model of surveillance is driven by the extraction of value (in the form of detailed information for the databases) from users – and historical experience dictates that where value is at stake, commercial interests are not self-limiting. Left to its own devices the market did not eliminate child labour, limit working hours or set

minimum wages. Nor will it set limits to data collection and sorting practices. These limits need to be determined collectively and imposed on the owners and operators of the databases. Thus, the report's call to improve, "the independent gathering of public opinion on a range of issues related to surveillance and data processing" (92) is a welcome one, as its emphasis on the importance of promoting public knowledge about surveillance issues (97). What control over productive resources was to the industrial revolution, control over communication and information resources will be to the digital era. Control over personal information is the database era analogue of control over labour power in the industrial revolution. Information, deliberation, and collective action will have crucial roles to play in what is certain to be an ongoing struggle.

References

- Ayres, I. 2007. *Super Crunchers: How Anything Can be Predicted*, London: John Murray.
- House of Lords Select Committee on the Constitution. 2009. *Surveillance: Citizens and the State*. London: Published by the Authority of the House of Lords.
- Lyon, D. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity.
- Secure Computing Magazine*. 2009. Surveillance Undermines Freedoms. 1 March, p. 10.
- States News Service*. 2009. Ever Increasing use of Surveillance and Data collection Risks Undermining Fundamental Freedoms. 6 February.
- Travis, A. 2009. Lords: Rise of CCTV is Threat to Freedom. *The Guardian*, 6 February, p. 1.
- The Times* (London). 2008. Your Views from Yesterday's Debates, October 7, p. 29.